Binary Block Coding

By S. P. LLOYD

(Manuscript received March 16, 1956)

From the work of Shannon one knows that it is possible to signal over an error-making binary channel with arbitrarily small probability of error in the delivered information. The effects of errors produced in the channel are to be eliminated, according to Shannon, by using an error correcting code. Shannon's proof that such codes exist does not provide a practical scheme for constructing them, however, and the explicit construction and study of such codes is of considerable interest.

Particularly simple codes in concept are the ones called here close packed strictly e-error-correcting (*the terminology is explained later*). *It is shown that for such a code to exist, not only must a condition due to Hamming be satisfied, but also another condition. The main result may be put as follows: a close-packed strictly e-error-correcting code on n, $n > e$, places cannot exist unless e of the coefficient vanish in $(1 + x)^e(1 - x)^{n-1-e}$ when this is expanded as a polynomial in x.*

I. INTRODUCTION

In this paper we investigate a certain problem in combinatorial analysis which arises in the theory of error correcting coding. A development of coding theory is to be found in the papers of Hamming[1] and Shannon[2]; this section is intended primarily as a presentation of the terminology used in subsequent sections.

We take (0, 1) as the range of binary variables. By an *n-word* we mean a sequence of n symbols, each of which is 0 or 1. We call the individual symbols of an n-word the *letters* of the n-word. We denote by B_n the set consisting of all the 2^n possible distinct n-words. The set B_n may be mapped onto the vertices of an n-dimensional cube, in the usual way, by regarding an n-word as an n-dimensional Cartesian coordinate expression. The *distance* $d(u, v)$ between n-words u and v is defined to be the number of places in which the letters of u and v differ; on the n-cube, this is seen to be the smallest number of edges in paths along edges between the vertices corresponding to u and v. The *weight* of an n-word u

is the number of 1's in the sequence u; it is the distance between u and the n-word $00\cdots0$, all of whose letters are 0.*

A *binary block code of size K on n places* is a class of K nonempty disjoint subsets of B_n where in each of the K sets a single n-word is chosen as the *code word* of the set.† Each such set is the *detection region* of the code word it contains, and we shall say that any n-word which falls in a detection region *belongs to* the code word of the detection region. The set consisting of those n-words which do not lie in any detection region we call *limbo*.‡ A *close packed* code is one for which limbo is an empty set; i.e., a code in which the deteetion regions constitute a partition (disjoint covering) of B_n .

A *sphere* of radius r centered at n-word u is the set $[v{:}d(u, v) \leqq r]$ of n-words v whicb differ from u in r or fewer places. A binary block code is *e-error-correcting* if each detection region includes tbe sphere of radius e centered at the code word of the detection region. We say that a binary block code is *strictly e-error-correeting* if each detection region is exactly the sphere of radius e centered at the code word of the detection region.

This paper is devoted to the consideration of close packed strictly e-error-correcting binary block codes. We shall refer to such a code as an *e-eode*, for brevity. Hamming[1] observes that a necessary condition for the existence of an e-code on n places is that

$$1 + n + \frac{1}{2}n(n-1) + \cdots + \binom{n}{e} \tag{1}$$

be a divisor of 2^n. In this paper we derive an additional necessary condition. Our condition includes as a special case a condition of Golay[4] for the existence of e-codes of group type, and applies to all e-codes, whether or not they are equivalent to group codes.§

* If B_n is regarded as a subset of the real linear vector spaee consisting of all sequences $\alpha = (\alpha_1, \alpha_2, \cdots, \alpha_n)$ of n real nnmbers, then the "weight" of an n-word is simply the ℓ_1 norm (defined as $\| \alpha \|_1 = \sum_1^n | \alpha_n |$), and our "distanee" is the metrie derived from this norm.

† The term "bloek eode", due to P. Elias, serves to distinguish the codes of fixed length considered here from the codes of unbounded delay introduced by Elias, Referenee 3.

‡ In a communications system[2] using suеh a code, the transmitter sends only eode words. If, due to errors in handling binary symbols, the receiver delivers itself of an n-word other than a code word then: (a) if the n-word lies in a detection region, one assumes that the eode word of the detection region was intended; (b) if the n-word lies in limbo, one makes a note to the effect that errors have oeeurred in handling the word but that one is not attempting to guess what they were.

§ The terms "gronp alphabet" (Slepian[5]), "systematie code" (Hamming[1]), "symbol code" (Golay[4]), "eheck symbol eode" (Elias[3]), "parity eheck code", are roughly synonymous. More precisely, a group eode is a parity eheek eode in which all of the parity check forms are homogeneous ("even"), so that $00\cdots0$ is one of the code words; see Reference 5.

11. DISTRIBUTION OF CODE WORDS

Suppose an e-code on n places is given. Let us inquire as to the distribution of weights of code words. We denote by ν_s the number of code words of weight s, $0 \leqq s \leqq n$, and by

$$G(x) = \sum_{s=0}^{n} \nu_s x^s \tag{2}$$

the generating function for these numbers, with x a complex but otherwise free variable. We show in this section that $G(x)$ satisfies a certain inhomogeneous linear differential equation of order e.

If there exists an e-code on n places then this differential equation will have $G(x)$ as a *polynomial* solution; the necessary condition for the existence of an e-code on n places given in Section 4 is essentially a restatement of this fact.* First, however, we must derive the differential equation and obtain its solutions.

If w_α is a code word of the given e-code ($1 \leqq \alpha \leqq K$), define the set of *j-neighbors of w_α* as the set of n-words which lie at distance exactly j from w_α; designate this set by $S_j(w_\alpha)$. ($S_0(w_\alpha)$ is the set whose only element is w_α itself.) Our derivation is based on the observation that, in an e-code on n places,

$$\bigcup_{\alpha=1}^{K} \bigcup_{j=0}^{e} S_j(w_\alpha) = B_n \dagger \tag{3}$$

is a partition of B_n. For, the detection regions:

$$\bigcup_{j=0}^{e} S_j(w_\alpha), \qquad 1 \leqq \alpha \leqq K$$

are disjoint, and in each such sum representing a detection region the summands are disjoint (the distance function being single valued). Furthermore, each n-word of B_n lies in some detection region (close packed property) and hence appears in one of the sets $S_j(w_\alpha)$ for some α and for some j satisfying $0 \leqq j \leqq e$.

The set

$$\bigcup_{\alpha=1}^{K} S_j(w_\alpha)$$

* The author is not yet able to demonstrate the converse. That is, suppose one obtains a polynomial solution $G(x)$ of (11), below, satisfying appropriate boundary conditions, and from it some coefficients ν_s, $0 \leqq s \leqq n$. It does not follow from the methods of this article that there is actually some e-code on n places for which these ν_s represent the number of code words of weight s.

† $\bigcup$ = set union.

consists of the n-words which are j-neighbors of some (not specified) code word; let us refer to these n-words simply as *j-neighbors*. Denote by $\nu_{j,s}$ the number of j-neighbors which are of weight s (with $\nu_{0,s} = \nu_s$, as above). Applying (3) to the n-words of weight s, we see that

$$\nu_s + \nu_{1,s} + \cdots + \nu_{e,s} = \binom{n}{s}, \qquad 0 \leqq s \leqq n \tag{4}$$

is the total number of n-words of weight s. If we multiply (4) by x^s and sum on s, we have

$$G(x) + G_1(x) + \cdots + G_e(x) = (1 + x)^n \tag{5}$$

where

$$G_j(x) = \sum_{s=0}^{n} \nu_{j,s} x^s \tag{6}$$

is the generating function (with respect to s) for the numbers $\nu_{j,s}$.

We now express $G_j(x)$, $0 \leqq j \leqq e$, in terms of $G(x)$. Suppose code word w is of weight s; that is, w consists of s ones and $n - s$ zeros in some order. A j-neighbor of w is obtained by choosing j places out of n and changing the letters of w in these places, 0's to 1's and 1's to 0's. If, in this procedure, q of the 1's of w are changed to 0's, so that $j - q$ of the 0's are changed to 1's, then the resulting j-neighbor of w is of weight $s - q + (j - q)$. Now, there are $\binom{s}{q}$ ways of choosing q places among the s where the letters of w are 1, and there are independently $\binom{n-s}{j-q}$ ways of choosing $j - q$ places among the $n - s$ where the letters of w are 0. Thus, of the $\binom{n}{j}$ different j-neighbors of w, the number $\binom{s}{q}\binom{n-s}{j-q}$ are of weight $s + j - 2q$. We may regard each of these as contributing $1 \cdot x^{s+j-2q}$ to the generating function $G_j(x)$ of (6) (provided $0 \leqq j \leqq e$, so that there is no overlap); hence, summing over all j-neighbors of a code word and then over all code words,

$$G_j(x) = \sum_{s=0}^{n} \nu_s \sum_{q=0}^{\infty} \binom{s}{q}\binom{n-s}{j-q} x^{s+j-2q} \qquad 0 \leqq j \leqq e \ * \tag{7}$$

From the easily verified polynomial identity

$$(x + y)^s(1 + xy)^{n-s} = \sum_{j=0}^{\infty} y^j \sum_{q=0}^{\infty} \binom{s}{q}\binom{n-s}{j-q} x^{s+j-2q}$$

* The limits $(0, \infty)$ on the q summation are merely for convenience; the binomial coefficients vanish outside the proper range, under the usual convention.

(n, s integers, $0 \leqq s \leqq n$) it follows that

$$\sum_{q=0}^{\infty} \binom{s}{q}\binom{n-s}{j-q} x^{s+j-2q} = \frac{1}{2\pi i}\int_C \frac{(x+y)^s(1+xy)^{n-s}}{y^{j+1}}\,dy$$

where contour C is, say, a small circle around the origin, taken positively. Thus

$$\begin{aligned} G_j(x) &= \sum_{s=0}^{n} \frac{\nu_s}{2\pi i}\int_C \frac{(x+y)^s(1+xy)^{n-s}}{y^{j+1}}\,dy \\ &= \frac{1}{2\pi i}\int_C \frac{(1+xy)^n}{y^{j+1}}\,G\left(\frac{x+y}{1+xy}\right)dy \qquad (8) \\ &\equiv L_jG(x) \end{aligned}$$

where the operator L_j is thus defined. Change of integration variable gives

$$\begin{aligned} L_jG(x) &= \frac{(1-x^2)^{n+1}}{2\pi i}\int_{C_x} \frac{G(z)\,dz}{(1-xz)^{n-j+1}(z-x)^{j+1}} \\ &= \frac{(1-x^2)^{n+1}}{j!}\,\frac{\partial^j}{\partial z^j}\,\frac{G(z)}{(1-xz)^{n-j+1}}\bigg|_{z=x} \qquad (9) \\ &= \sum_{p=0}^{j}\binom{n-p}{j-p}\frac{x^{j-p}(1-x^2)^p}{p!}\,\frac{d^pG(x)}{dx^p} \end{aligned}$$

(with C_x a small circle enclosing x but not x^{-1}, $x^2 \neq 1$). Thus L_j may be regarded as a linear differeutial operator of order j, ($L_0 \equiv 1$).

Using this result, (5) may be given the form

$$\begin{aligned} (1+x)^n &= [L_0 + L_1 + \cdots + L_e]G(x) \\ &= \frac{1}{2\pi i}\int_C \frac{y^{-e-1}-1}{1-y}\,(1+xy)^nG\left(\frac{x+y}{1+xy}\right)dy \qquad (10) \\ &\equiv MG(x) \end{aligned}$$

this last expression as a definition of operator M. Written as a differential equation, (10) is

$$\sum_{p=0}^{e}\frac{(1-x^2)^p}{p!}\sum_{r=0}^{e-p}\binom{n-p}{r}x^r\,\frac{d^pG(x)}{dx^p} = (1+x)^n \qquad (11)$$

It is straightforward that the only singularities of this equation are regular singularities[5] at $x = \pm 1, \infty$.

III. THE DIFFERENTIAL EQUATION

In this section we discuss (11) without reference to the fact that $G(x)$ is supposed to be a generating function. That is to say, with n and e

fixed but arbitrary non-negative integers, we denote by

$$G(x) = \sum_{s=0}^{\infty} \nu_s x^s \tag{12}$$

any solution of (11) regular in the unit circle.

It proves convenient to introduce certain functions $f_{n,\xi}(x)$ defined by

$$\begin{aligned} f_{n,\xi}(x) &\equiv (1 + x)^{\xi}(1 - x)^{n-\xi} \\ &= \sum_{s=0}^{\infty} \varphi_s(n, \xi) x^s \end{aligned} \tag{13}$$

where the coefficients $\varphi_s(n, \xi)$ are given by

$$\varphi_s(n, \xi) = \sum_{r=0}^{s} (-1)^r \binom{n - \xi}{r} \binom{\xi}{s - r} \tag{14}$$

Here, ξ is to be regarded as a free complex variable. By $(1 + x)^{\xi}(1 - x)^{n-\xi}$ we mean $\exp(\xi \log(1 + x) + (n - \xi) \log(1 - x))$, each logarithm vanishing at $x = 0$. As a function of x this function is single valued in, say, the x-plane cut on $(-\infty, -1]$ and $[1, \infty)$, and the series (13) converges to it in: $|x| < 1$.

Binomial coefficients are defined by

$$\begin{aligned} \binom{\zeta}{s} &\equiv \frac{\Gamma(\zeta + 1)}{s!\Gamma(\zeta + 1 - s)} \\ &= \frac{\zeta(\zeta - 1) \cdots (\zeta - s + 1)}{s!} \qquad s > 0 \end{aligned}$$

when ζ is not an integer, and $\varphi_s(n, \xi)$ is seen to be a polynomial in ξ of degree s:

$$\varphi_s(n, \xi) = \frac{2^s}{s!} \xi^s + \cdots + (-1)^s \binom{n}{s} \tag{15}$$

The recurrence relation

$$\varphi_0(n, \xi) + \varphi_1(n, \xi) + \cdots + \varphi_s(n, \xi) = \varphi_s(n - 1, \xi) \tag{16}$$

obtained by expanding the various factors [ ] in the identity

$$[(1 + x)^{\xi}(1 - x)^{n-\xi}][(1 - x)^{-1}] = [(1 + x)^{\xi}(1 - x)^{n-1-\xi}]$$

is an important one. We note also for reference that

$$\begin{aligned} \varphi_0(n, \xi) &= 1 \\ \varphi_s(n, n - \xi) &= (-1)^s \varphi_s(n, \xi) \\ \varphi_s(n, n) &= \binom{n}{s} \\ \varphi_s(n - 1, n) &= 1 + \binom{n}{1} + \cdots + \binom{n}{s} \end{aligned} \tag{17}$$

valid for all n, ξ and non-negative integers s. We see, by the way, that $\varphi_e(n-1, n)$ is simply the Hamming expression (1).

The function $f_{n,\xi}(x)$ has the property that

$$f_{n,\xi}\left(\frac{x+y}{1+xy}\right) = \frac{f_{n,\xi}(x)f_{n,\xi}(y)}{(1+xy)^n} \tag{18}$$

at least if, say, given x, $|y|$ is small enough. From this and (8) for the operator L_j it is apparent that

$$L_j f_{n,\xi}(x) = \varphi_j(n, \xi) f_{n,\xi}(x) \tag{19}$$

Similarly, using (19) and (16), or directly from (10) for the operator M,

$$\begin{aligned} Mf_{n,\xi}(x) &= [L_0 + L_1 + \cdots + L_e]f_{n,\xi}(x) \\ &= \varphi_e(n-1, \xi)f_{n,\xi}(x) \end{aligned} \tag{20}$$

If ξ_β is one of the roots of the polynomial $\varphi_e(n-1, \xi)$ then (20) becomes

$$M(1+x)^{\xi_\beta}(1-x)^{n-\xi_\beta} = 0$$

If we assume for the moment for simplicity that $\varphi_e(n-1, \xi)$ has e *distinct* roots ξ_β, $1 \leqq \beta \leqq e$, then (11) has as complementary function

$$\sum_{\beta=1}^{e} A_\beta(1+x)^{\xi_\beta}(1-x)^{n-\xi_\beta}$$

where the A_β are e arbitrary constants.

Fortunately, the function $(1+x)^n = f_{n,n}(x)$ is also a member of the family (13); hence

$$M(1+x)^n = \varphi_e(n-1, n)(1+x)^n$$

and the function

$$\frac{(1+x)^n}{\varphi_e(n-1, n)}$$

is a particular integral of (11). [We see from (17) that $\varphi_e(n-1, n)$ does not vanish in cases of interest.] Finally, when the roots of $\varphi_e(n-1, \xi)$ are distinct, the general solution of (11) must be of the form

$$G(x) = \frac{(1+x)^n}{\varphi_e(n-1, n)} + \sum_{\beta=1}^{e} A_\beta(1+x)^{\xi_\beta}(1-x)^{n-\xi_\beta} \tag{21}$$

If $\varphi_e(n-1, \xi)$ has multiple roots then the general solution will contain additional terms

$$(\text{const.})\ (1+x)^{\xi_\beta}(1-x)^{n-\xi_\beta}\left[\log\frac{1+x}{1-x}\right]^\mu \tag{22}$$

i.e., the μ^{th} derivative of $f_{n,\xi}(x)$ with respect to ξ, with μ any positive integer less than the multiplicity of root ξ_β.

Before applying these results to e-codes in detail, let us derive a certain modification of (21). First, we see from (17) that if n is a positive integer, then n is not one of the roots of $\varphi_e(n-1, \xi)$. If the roots ξ_β of $\varphi_e(n-1, \xi)$ are distinct and if A_β, $1 \leqq \beta \leqq e$, are any e numbers then a polynomial $\theta(\xi)$ of formal degree e is uniquely determined by the $e+1$ conditions:

$$\begin{aligned} \theta(\xi_\beta) &= (\xi_\beta - n)\varphi_e'(n-1, \xi_\beta)A_\beta, \qquad 1 \leqq \beta \leqq e,^* \\ \theta(n) &= 1 \end{aligned} \tag{23}$$

using, e.g., the Lagrange interpolation formula. It is obvious that $G(x)$, (2t), may be expressed in terms of this polynomial as

$$G(x) = \frac{1}{2\pi i}\int_\Gamma \frac{(1+x)^\xi(1-x)^{n-\xi}\theta(\xi)}{(\xi - n)\varphi_e(n-1, \xi)}\,d\xi \tag{24}$$

where Γ is any simple closed contour surrounding the roots: $n, \xi_1, \xi_2, \cdots, \xi_e$ of the denominator of the integrand; (the numerator is an entire function of ξ provided $x^2 \neq 1$).

Analysis a little more detailed shows that even if $\varphi_e(n-1, \xi)$ has multiple roots the general solution of (11) can be represented in the form (24), again with $\theta(\xi)$ any polynomial of formal degree e such that $\theta(n) = 1$. The e constants of integration appear as the $e+1$ parameters of $\theta(\xi)$ restricted by $\theta(n) = 1$.†

Expansion of the integrand in (24) according to (13) yields the form

$$\nu_s = \frac{1}{2\pi i}\int_\Gamma \frac{\varphi_s(n, \xi)\theta(\xi)}{(\xi - n)\varphi_e(n-1, \xi)}\,d\xi \qquad s = 0, 1, 2, \cdots \tag{25}$$

for the coefficients of $G(x)$, (12).

If we denote by

$$L_jG(x) \equiv G_j(x) = \sum_{s=0}^{\infty} \nu_{j,s}x^s \tag{26}$$

the result of applying the operator L_j to any solution (24) of (11), then it is straightforward that

$$G_j(x) = \frac{1}{2\pi i}\int_\Gamma \frac{(1+x)^\xi(1-x)^{n-\xi}\varphi_j(n, \xi)\theta(\xi)}{(\xi - n)\varphi_e(n-1, \xi)}\,d\xi, \tag{27}$$

* The prime denotes differentiation with respect to ξ.

† If $G(x)$ of (24) is to satisfy (11) it is sufficient that $\theta(\xi)$ be any function regular within (and on) Γ and that $\theta(n) = 1$, as may be easily verified. Since $G(x)$ depends on $\theta(\xi)$ only by way of the values of $\theta(\xi)$ at the zeros of the denominator in (24), the condition that $\theta(\xi)$ be a polynomial of formal degree e serves merely to determine $\theta(\xi)$ uniquely for a given solution $G(x)$.

and that

$$\nu_{j,s} = \frac{1}{2\pi i}\int_\Gamma \frac{\varphi_s(n,\xi)\varphi_j(n,\xi)\theta(\xi)}{(\xi - n)\varphi_e(n-1,\xi)}\,d\xi, \qquad s = 0, 1, \cdots \tag{28}$$

(An interesting reciprocity $\nu_{j,s} = \nu_{s,j}$ is apparent from (28). In an e-code one has (number of j-neighbors of weight s) = (number of s-neighbors of weight j) only for $0 \leqq s, j \leqq e$, since $L_jG(x)$ is the generating function for j-neighbors only if $0 \leqq j \leqq e$.)

IV. BOUNDARY CONDITIONS

The coefficients ν_s, (25), of any solution of (11) satisfy the relation:

$$\nu_0 + \nu_1 + \cdots + \nu_e = \frac{1}{2\pi i}\int_\Gamma \frac{\theta(\xi)}{\xi - n}\,d\xi = 1 \tag{29}$$

by virtue of (16) and the normalizing condition $\theta(n) = 1$.

With γ an integer such that $0 \leqq \gamma \leqq e$, denote by

$$G^{(\gamma)}(x) = \sum_{s=0}^{\infty} \nu_s{}^{(\gamma)} x^s \tag{30}$$

a solution of (11) which satisfies the e boundary conditions

$$\begin{aligned} \nu_0{}^{(\gamma)} &= \nu_1{}^{(\gamma)} = \cdots = \nu_{\gamma-1}{}^{(\gamma)} = 0 \\ \nu_{\gamma+1}{}^{(\gamma)} &= \nu_{\gamma+2}{}^{(\gamma)} = \cdots = \nu_e{}^{(\gamma)} = 0 \end{aligned} \tag{31}$$

We must have $\nu_\gamma{}^{(\gamma)} = 1$ in such a solution, from (29). Thus the conditions (31) are equivalent to specifying the values of $G^{(\gamma)}(x)$ and its first $e - 1$ derivatives at the ordinary point $x = 0$ of (11), so that such a solution $G^{(\gamma)}(x)$ exists and is uniquely determined.[6]

Given an e-code on n places, each n-word of B_n lies at distance e or less from exactly one code word; namely, the code word to which it belongs. In particular, the n-word $00\cdots0$ must lie at distance e or less from a single code word. That is to say, there is exactly one code word in the sphere of radius e centered at $00\cdots0$. If this code word is of weight γ, then the generating function for the given e-code can be none other than the solution $G^{(\gamma)}(x)$ of (11) defined in the preceding paragraph.

If there exists an e-code on n places in which the code word of least weight is of weight γ, then there can be derived from it an e-code on n places in which the code word of least weight is of weight γ', where γ' is any integer satisfying $0 \leqq \gamma' \leqq e$. The transformation is that of choosing certain places among n and then changing the letters of each n-word of B_n in these places, 0's to 1's and 1's to 0's. (Such a transformation

corresponds to one of the operations of the orthogonal group which leaves invariant the n-cube representing B_n .) Metric properties in B_n are invariant under such a transformation, clearly, and an e-code is transformed into an e-code. Thus if there exists any e-code on n places then (11) must have $e + 1$ distinct polynomial solutions $G^{(\gamma)}(x)$, satisfying boundary conditions (31) for each case $\gamma = 0, 1, \cdots, e$.

In (25) for the coefficients ν_s , move contour Γ out to a circle sufficiently large that the expansion

$$\frac{1}{(\xi - n)\varphi_e(n-1,\xi)} = \frac{e!}{2^e\xi^{e+1}} + \frac{(\text{const.})}{\xi^{e+2}} + \cdots$$

converges on Γ. Suppose that the polynomial $\theta(\xi)$, of formal degree e, is of actual degree f: $\theta(\xi) = c\xi^f + 0(\xi^{f-1})$, $c \neq 0$, where $0 \leqq f \leqq e$. Then the numerator of the integrand in (25) is of the form: $(2^s c\xi^{s+f}/s!) + 0(\xi^{s+f-1})$, and it is clear that

$$\nu_s = 0 \qquad 0 \leqq s \leqq e - f - 1$$

$$\nu_{e-f} = \frac{e!c}{2^f(e-f)!} \neq 0$$

Hence, if $\theta^{(\gamma)}(\xi)$ denotes the polynomial which gives $G^{(\gamma)}(x)$ in the representation (24), then $\theta^{(\gamma)}(\xi)$ must be of actual degree $e - \gamma$.

A particularly simple case is the one $\gamma = e$; the polynomial $\theta^{(e)}(\xi)$ must be of degree zero, and is determined by the normalization as $\theta^{(e)}(\xi) \equiv 1$. Thus

$$G^{(e)}(x) = \frac{1}{2\pi i}\int_\Gamma \frac{(1+x)^\xi(1-x)^{n-\xi}}{(\xi - n)\varphi_e(n-1,\xi)}\,d\xi \tag{32}$$

From this we have immediately the following

Theorem: If there exists an e-code on n places then the equation $\varphi_e(n-1,\xi) = 0$ in ξ has e distinct integer roots.

Proof: If there exists an e-code on n places, then there exists an e-code on n places in which the code word of least weight is of weight e. The solution (32) of (11) must be the generating function for this e-code; hence (32) must reduce to a polynomial of formal degree n. If $\varphi_e(n-1,\xi)$ had multiple roots then noncancelling logarithmic terms (22) would appear in the $G^{(e)}(x)$ of (32). Thus $\varphi_e(n-1,\xi)$ must have e distinct roots ξ_β , $1 \leqq \beta \leqq e$. Each solution $(1+x)^{\xi_\beta}(1-x)^{n-\xi_\beta}$ of the homogeneous equation appears in $G^{(e)}(x)$ with nonvanishing coefficient:

$$A_\beta = \frac{1}{(\xi_\beta - n)\varphi_e'(n-1,\xi_\beta)}$$

Since $G^{(e)}(x)$ must be a polynomial in x, it must be expressible as a polynomial in $1 + x$; hence each root ξ_β must be an integer.* (It is not necessary to require further that $0 \leqq \xi_\beta \leqq n$, since it follows easily from (14) that any real root of $\varphi_e(n - 1, \xi)$ satisfies $0 \leqq \xi_\beta \leqq n - 1$ provided n and e are integers such that $0 \leqq e \leqq n$.)

As a corollary we have that if e is odd then n must be odd. This follows from the theorem and the fact that $\frac{1}{2}(n - 1)$ is a root of $\varphi_e(n - 1, \xi)$ when e is odd, from (17).

We consider next the case $\gamma = 0$. If $00\cdots0$ is a code word, then its e-neighbors are the n-words of weight e. Furthermore, the n-words of weight less than e belong to the code word $00\cdots0$, and can be e-neighbors neither of $00\cdots0$ nor of any other code word. Hence it must be true that

$$G_e^{(0)}(x) = \binom{n}{e} x^e + 0(x^{e+1}) \tag{33}$$

With $G_e^{(0)}(x)$ represented in the form (27), divide the factor $\varphi_e(n, \xi)\theta^{(0)}(\xi)$ in the numerator by the denominator; the result will be

$$\varphi_e(n, \xi)\theta^{(0)}(\xi) = [(\xi - n)\varphi_e(n - 1, \xi)]q(\xi) + r(\xi) \tag{34}$$

with quotient $q(\xi)$ a polynomial of degree $e - 1$ and remainder $r(\xi)$ a polynomial of formal degree e. The term involving $q(\xi)$ obviously contributes nothing to $G_e^{(0)}(x)$ in (27), so that from (33) and arguments similar to those giving $G^{(e)}(x)$, above, $r(\xi)$ must be the constant

$$r(\xi) = \binom{n}{e} = \varphi_e(n, n)$$

From (34) we then obtain the values of $\theta^{(0)}(\xi)$ at the poles of the integrand in (24), and thus

$$G^{(0)}(x) = \frac{(1 + x)^n}{\varphi_e(n - 1, n)} + \sum_{\beta=1}^{e} \frac{\varphi_e(n, n)(1 + x)^{\xi_\beta}(1 - x)^{n-\xi_\beta}}{\varphi_e(n, \xi_\beta)(\xi_\beta - n)\varphi_e'(n - 1, \xi_\beta)} \tag{35}$$

Before obtaining $G^{(\gamma)}(x)$ explicitly for intermediate values of γ, we must first discuss a certain set of recursion relations holding between the coefficients ν_s of any solution of (11). These relations are

$$\sum_{s=e-\rho+1}^{e+\rho} (-1)^{e+s} k_{\rho,s} \nu_s = 0, \quad \rho = 1, 2, \cdots, \tag{36}$$

* The condition of Golay for the existence of group codes, obtained by different means, is essentially that $\varphi_e(n - 1, \xi)$ have at least one root an integer. Cf.: (4) of Reference 4, in view of (16), above.

where we define $\nu_s = 0$ for $s < 0$ and where the coefficients $k_{\rho,s}$ are

$$k_{\rho,s} = \sum_{\sigma=0}^{\rho} \binom{s}{\sigma}\binom{n-s}{\rho-\sigma}\binom{\rho-1}{e-s+\sigma} \tag{37}$$

(The derivation of (36) is given in Appendix A.) Equations (36), written out, are of the form

$$k_{1,\,e}\nu_e - k_{1,\,e+1}\nu_{e+1} = 0$$
$$k_{2,\,e-1}\nu_{e-1} - k_{2,\,e}\nu_e + k_{2,\,e+1}\nu_{e+1} - k_{2,\,e+2}\nu_{e+2} = 0$$
$$\vdots$$

from which we see that (36) may be used to determine

$$\nu_{e+1}\,,\ \nu_{e+2}\,,\ \cdots$$

recursively in terms of

$$\nu_e\,,\ \nu_{e-1}\,,\ \cdots\,,\ \nu_0$$

We see also that if

$$\nu_e = \nu_{e-1} = \cdots = \nu_{\gamma+1} = 0$$

(with γ such that $0 \leqq \gamma \leqq e-1$) then

$$\nu_{e+1} = \nu_{e+2} = \cdots = \nu_{2e-\gamma} = 0.$$

This has the following interpretation in terms of e-codes. It is well known (and obvious) that two different code words in an e-code must be separated by distance at least $2e+1$. Hence if the code word of least weight in an e-code is of weight γ then all other code words are of weight not less than $2e+1-\gamma$. In the generating function for such a code it must be the case that not only

$$G^{(\gamma)}(x) = x^\gamma + 0(x^{e+1})$$

but in fact

$$G^{(\gamma)}(x) = x^\gamma + 0(x^{2e+1-\gamma}) \tag{38}$$

Equations (36) insure that this condition is satisfied automatically.*

As a particular case of (38), we have

$$G^{(0)}(x) = 1 + 0(x^{2e+1}).$$

We see that if we apply the operator L_γ to $G^{(0)}(x)$ there will result

$$L_\gamma G^{(0)}(x) = \varphi_\gamma(n,n)x^\gamma + 0(x^{2e+1-\gamma}) \tag{39}$$

* It is also necessary for the existence of an e-code that (36) determine $\nu_{e+1}\,,\ \nu_{e+2}\,,\ \cdots$ as non-negative integers when $\nu_e\,,\ \nu_{e-1}\,,\ \cdots\,,\ \nu_0$ are those of (31). This condition is discussed a little further in Appendix A.

using the differential operator form for L_γ, (9). On the other hand, the function

$$\frac{L_\gamma G^{(0)}(x)}{\varphi_\gamma(n, n)} = \frac{1}{2\pi i}\int_\Gamma \frac{(1+x)^\xi(1-x)^{n-\xi}}{(\xi - n)\varphi_e(n-1, \xi)}\left[\frac{\theta^{(0)}(\xi)\varphi_\gamma(n, \xi)}{\varphi_\gamma(n, n)}\right] d\xi \quad (40)$$

is a solution of differential equation (11), in view of the discussion following (24). From (39) we see that this function can be none other than $G^{(\gamma)}(x)$. Finally, applying L_γ to $G^{(0)}(x)$ in the form (35), we have explicitly

$$G^{(\gamma)}(x) = \frac{(1+x)^n}{\varphi_e(n-1, n)} + \frac{\varphi_e(n, n)}{\varphi_\gamma(n, n)}\sum_{\beta=1}^{e} \frac{\varphi_\gamma(n, \xi_\beta)(1+x)^{\xi_\beta}(1-x)^{n-\xi_\beta}}{\varphi_e(n, \xi_\beta)(\xi_\beta - n)\varphi_e'(n-1, \xi_\beta)} \quad 0 \le \gamma \le e. \quad (41)$$

V. EXAMPLES

The known cases where the condition of Hamming is satisfied are the following:

Case I: $e = 0, n \ge 1$

The Hamming expression (1) reduces to unity. In fact,

$$\varphi_0(n-1, \xi) \equiv 1,$$

and the condition that all roots be integers is vacuous. The generating function for code words is (uniquely):

$$G^{(0)}(x) = \frac{(1+x)^n}{\varphi_0(n-1, n)} = (1+x)^n$$

Each n-word of B_n is a detection region and thus a code word. There is no error correction.

Case II: $e \ge 1, n = e$

The Hamming expression becomes the sum of all the terms in the binomial expansion of $(1+1)^n$. The "codes" in this class consist of a single code word surrounded by its detection region consisting of the sphere B_n of radius n. No signalling is possible, of course, but our methods still apply.

From the representation

$$\varphi_s(n, \xi) = \frac{1}{2\pi i}\int_c \frac{(1+x)^\xi(1-x)^{n-\xi}}{x^{s+1}}\,dx = \frac{1}{2\pi i}\int_c \frac{(1+2v)^\xi}{v^{s+1}(1+v)^{n-s+1}}\,dv \quad (42)$$

(valid for all n, ξ) we have immediately

$$\varphi_n(n-1,\xi) = 2^n\binom{\xi}{n} = \frac{2^n}{n!}\xi(\xi-1)\cdots(\xi-n+1)$$

and the roots are $0, 1, \cdots, n-1$. The generating function $G^{(e)}(x)$ of (32) becomes*

$$\begin{aligned} G^{(n)}(x) &= \frac{n!}{2^n}\cdot\frac{1}{2\pi i}\int_\Gamma \frac{(1+x)^\xi(1-x)^{n-\xi}}{(\xi)_{n+1}}\,d\xi \\ &= \frac{n!}{2^n}\sum_{\xi=0}^{n}\frac{(-1)^{n-\xi}}{\xi!(n-\xi)!}(1+x)^\xi(1-x)^{n-\xi} \\ &= \frac{1}{2^n}[(1+x)-(1-x)]^n = x^n \end{aligned}$$

as one might expect. The explicit form for $\varphi_n(n,\xi)$ is somewhat complicated, but for ξ an integer it follows immediately from definition (13) that

$$\varphi_n(n,\xi) = (-1)^{n-\xi} \qquad \xi = 0, 1, \cdots, n$$

From (35), then,

$$\begin{aligned} G^{(0)}(x) &= \frac{1}{2^n}\sum_{\xi=0}^{n}\binom{n}{\xi}(1+x)^\xi(1-x)^{n-\xi} \\ &= \frac{1}{2^n}[(1+x)+(1-x)]^n = 1 \end{aligned}$$

which, again, is not surprising. The details for other values of γ seem to be more tedious, although one expects (41) to yield $G^{(\gamma)}(x) = x^\gamma$.

Case III: $e \geqq 1$, $n = 2e+1$

The Hamming expression in this case:

$$1 + \binom{2e+1}{1} + \cdots + \binom{2e+1}{e} = 2^{2e}$$

consists of the first half of the terms in the binomial expansion of $(1+1)^{2e+1}$. The code words in a code of this class are any two n-words separated by distance n (i.e., two vertices at opposite corners of the n-cube). The group codes in this class are the "majority rule" codes.† From (42) we have (using the substitution $y = 4v + 4v^2$)

* $(\xi)_s \equiv s!\binom{\xi}{s}$ denotes the descending factorial.

† The two code words in such a code are $00\cdots0$ and $11\cdots1$. An n-word belongs to $00\cdots0$ if it contains more 0's than 1's, and to $11\cdots1$ if it contains more 1's than 0's.

$$\varphi_s(n, \xi) = \frac{2^n}{2\pi i}\int_c \frac{(1+y)^{\frac{1}{2}(\xi-1)}\,dy}{[(1+y)^{\frac{1}{2}}-1]^{s+1}[(1+y)^{\frac{1}{2}}+1]^{n-s+1}}, \qquad (43)$$

and, without difficulty,

$$\varphi_e(2e, \xi) = 2^{2e}\binom{\frac{1}{2}(\xi-1)}{e} = \frac{2^e}{e!}(\xi-1)(\xi-3)\cdots(\xi-2e+1)$$

The roots are $1, 3, \cdots, 2e-1$, and from (32):

$$\begin{aligned} G^{(e)}(x) &= \frac{e!}{2^e}\cdot\frac{1}{2\pi i}\int_{\mathrm{r}} \frac{(1+x)^{\xi}(1-x)^{2e+1-\xi}\,d\xi}{(\xi-2e-1)(\xi-1)(\xi-3)\cdots(\xi-2e+1)} \\ &= 2^{-2e}(1+x)(1+x)^2-(1-x)^2]^e = x^e + x^{e+1} \end{aligned}$$

In the case $\gamma = 0$ we need the result

$$\varphi_e(2e+1, \xi) = 2^{2e+1}\left[\binom{\frac{1}{2}\xi}{e+1} - \binom{\frac{1}{2}(\xi-1)}{e+1}\right]$$

from (43). It is then tedious but straightforward to obtain from (35)

$$\begin{aligned} G^{(0)}(x) &= \frac{1}{2^{2e}}\sum_{r=0}^{e}\binom{2e+1}{2r+1}(1+x)^{2r+1}(1-x)^{2e-2r} \\ &= 2^{-2e-1}\{[(1-x)+(1+x)]^{2e+1} - [(1-x)-(1+x)]^{2e+1}\} \\ &= 1 + x^{2e+1} \end{aligned}$$

One expects to get

$$G^{(\gamma)}(x) = x^{\gamma} + x^{2e+1-\gamma}$$

from (41), but verification appears to be complicated.

Case IV: $e = 1$, $n = 2^t - 1$ $(t = 3, 4, \cdots)$

The single error correcting codes of Hamming[1] are included here. (The examples for $t = 1$, resp. $t = 2$, appear under Case II, resp. Case III, above.) Since n is always odd the condition that $\varphi_1(n-1, \xi) = 2\xi - n + 1$ have an integer root is automatically satisfied. For $\gamma = 1$ the generating function is

$$\begin{aligned} G^{(1)}(x) &= \frac{1}{2\pi i}\int_{\mathrm{r}} \frac{(1-x)^{\xi}(1-x)^{n-\xi}}{(\xi-n)(2\xi-n+1)}\,d\xi \\ &= \frac{(1+x)^n - (1+x)^{\frac{1}{2}(n-1)}(1-x)^{\frac{1}{2}(n+1)}}{1+n} \end{aligned}$$

from which we have

$$\nu_s^{(1)} = \frac{1}{1+n}\left\{\binom{n}{s} - (-1)^{\frac{1}{2}s}\binom{\frac{1}{2}(n-1)}{\frac{1}{2}s}\right\} \quad s \text{ even}$$

$$\nu_s^{(1)} = \frac{1}{1+n}\left\{\binom{n}{s} - (-1)^{\frac{1}{2}(s+1)}\binom{\frac{1}{2}(n-1)}{\frac{1}{2}(s-1)}\right\} \quad s \text{ odd}$$

For $\gamma = 0$, Eq. (35) works out as

$$G^{(0)}(x) = \frac{(1+x)^n + n(1+x)^{\frac{1}{2}(n-1)}(1-x)^{\frac{1}{2}(n+1)}}{1+n}$$

so that

$$\nu_s^{(0)} = \frac{1}{1+n}\left\{\binom{n}{s} + n(-1)^{\frac{1}{2}s}\binom{\frac{1}{2}(n-1)}{\frac{1}{2}s}\right\} \quad s \text{ even}$$

$$\nu_s^{(0)} = \frac{1}{1+n}\left\{\binom{n}{s} + n(-1)^{\frac{1}{2}(s+1)}\binom{\frac{1}{2}(n-1)}{\frac{1}{2}(s-1)}\right\} \quad s \text{ odd}$$

Case V: $e = 2$, $n = 90$

The double error correcting codes for $n = 2, 5$ are covered by Cases II, III, respectively. The discovery that

$$1 + 90 + \tfrac{1}{2}(90)(89) = 2^{12}$$

is due to Golay.[7] We have

$$2\varphi_2(n-1, \xi) = (2\xi - n + 1)^2 - (n-1)$$

with roots

$$\tfrac{1}{2}[n - 1 \pm (n-1)^{\frac{1}{2}}]$$

Since these roots are not integers when $n = 90$, there can be no 2-code for $n = 90$.* H. S. Shapiro has shown (in unpublished work) that the Hamming condition for $e = 2$ is satisfied only in the cases $n = 2, 5, 90$, so that the only nontrivial 2-codes are those equivalent to the majority rule code on 5 places.

Case VI: $e = 3$, $n = 23$

Golay[7] finds:

$$1 + 23 + \tfrac{1}{2}(23)(22) + (23)(22)(21)/6 = 2^{11}$$

and gives explicitly a 3-code on 23 places of group type. We have

$$6\varphi_3(n-1, \xi) = (2\xi - n + 1)[(2\xi - n + 1)^2 - (3n - 5)]$$

and when $n = 23$ we verify that the roots are the integers 7, 11, 15. Computations by the author show that for $n < 10^{10}$ the Hamming condition for $e = 3$ holds only when $n = 3, 7, 23$.

* This settles a question raised by Golay, who shows that there is no code of group type in this case, but not that there is no code at all.

For $e = 4$ we have

$$24\varphi_4(n - 1, \xi) = [(2\xi - n + 1)^2 - (3n - 7)]^2 - (6n^2 - 30n + 40)$$

For $n = 4, 9$ this reduces to the forms given under Cases II, III. Preliminary calculations by the author shows that any other solutions of the Hamming condition for $e = 4$ must be such that $n > 10^{10}$, so that the question of the existence of 4-codes (other than the majority rule code) is somewhat academic.

Computations of Mrs. G. Rowe of the Mathematical Research Department show that Cases I–VI cover all cases of the Hamming condition being satisfied in the range

$$0 \leqq e \leqq n, \qquad 1 \leqq n \leqq 150$$

Appendix A

From (13) we have

$$\left(\frac{1 - x}{1 + x}\right)^{n-\xi} = \frac{1}{(1 + x)^n} \sum_{s=0}^{\infty} \varphi_s(n, \xi)x^s \tag{A1}$$

Applying the operator $D = -(1 + x)^2 d/dx$ to both sides of (A1) ρ times, there results

$$2^\rho(n - \xi)_\rho \left(\frac{1 - x}{1 + x}\right)^{n-\xi-\rho} = \sum_{s=0}^{\infty} \varphi_s(n, \xi)D^\rho[x^s(1 + x)^{-n}] \tag{A2}$$

The substitution $v = (1 + x)^{-1}$ reduces D to d/dv, so that

$$\begin{aligned} D^\rho x^s(1 + x)^{-n} &= \frac{d^\rho}{dv^\rho}(1 - v)^s v^{n-s} \\ &= \sum_{\sigma=0}^{\rho} \binom{\rho}{\sigma} (-1)^\sigma (s)_\sigma (1 - v)^{s-\sigma}(n - s)_{\rho-\sigma} v^{n-s-\rho+\sigma} \\ &= \rho! \sum_{\sigma=0}^{\rho} (-1)^\sigma \binom{s}{\sigma}\binom{n - s}{\rho - \sigma} x^{s-\sigma}(1 + x)^{\rho-n} \end{aligned}$$

using Leibnitz's rule. We substitute this into Eq. (A2), multiply both sides of the result by

$$(1 + x)^{n-\rho}(1 - x)^{\rho-\tau}/\rho!$$

(with τ arbitrary), and then equate coefficients of x^t on both sides; there obtains

$$2^\rho \binom{n - \xi}{\rho} \varphi_t(n - \tau, \xi) = \sum_{s=0}^{t+\rho} (-1)^{t+s} \kappa_{\rho,s}(n, \tau; t)\varphi_s(n, \xi) \tag{A3}$$

valid for all n, ξ, τ and all non-negative integers ρ, t, where

$$\kappa_{\rho,s}(n, \tau; t) = \sum_{\sigma=0}^{\rho} \binom{s}{\sigma}\binom{n-s}{\rho-\sigma}\binom{\rho-\tau}{t-s+\sigma} \tag{A4}$$

The coefficients $\kappa_{\rho,s}(n, \tau; t)$ vanish unless $s \leqq t + \rho$; if n and $\rho - \tau$ are non-negative integers then the coefficients $\kappa_{\rho,s}(n, \tau; t)$ are positive integers provided $t - \rho + \tau \leqq s$ and vanish otherwise. In particular, (setting $\tau = 1$, $t = e$),

$$2^{\rho}\binom{n-\xi}{\rho}\varphi_e(n-1, \xi) = \sum_{s=e-\rho+1}^{e+\rho} (-1)^{e+s} k_{\rho,s}\varphi_s(n, \xi), \rho = 1, 2, \cdots, \tag{A5}$$

where we define $\varphi_s(n, \xi) \equiv 0$ for $s < 0$; the $k_{\rho,s} = \kappa_{\rho,s}(n, 1; e)$ are those of (37) of the text. If we multiply ν_s of (25) by $(-1)^{e+s}k_{\rho,s}$ and sum on s there results (36), since the left hand member of (A5) is a polynomial multiple of the denominator of the integrand in (25).

If the code word of least weight in an e-code is of weight γ, then the first nontrivial one of the (37) is the one for $\rho = e + 1 - \gamma$, and it gives (since $\nu_\gamma^{(\gamma)} = 1$)

$$\begin{aligned}\nu_{2e+1-\gamma}^{(\gamma)} &= \frac{k_{e+1-\gamma,\gamma}}{k_{e+1-\gamma,2e+1-\gamma}} \\ &= \frac{(n-\gamma)(n-\gamma-1)\cdots(n-e)}{(2e+1-\gamma)(2e-\gamma)\cdots(e+1)}\end{aligned}$$

A necessary condition for the existence of au e-code on n places is that this expression be a non-negative integer in each case $\gamma = 0, 1, \cdots, e$. It is not clear, however, that this condition is independent of the one set forth in the theorem of Section IV.

Appendix B

We give here a relation due to K. M. Case[8] which shows that the statement of our main result as it appears in the Abstract heading this article agrees with the theorem proved in Section IV.

In the defining relation

$$(1 + x)^r(1 - x)^{n-r} = \sum_{s=0}^{\infty} x^s\varphi_s(n, r) \tag{B1}$$

for the coefficients $\varphi_s(n, r)$ assume that n and r are integers, multiply both sides by $(-1)^r\binom{n}{r}y^r$, and sum on r, $0 \leqq r \leqq n$. The result is

$$[(1 - x) - y(1 + x)]^n = \sum_{r=0}^{n}\sum_{s=0}^{n} (-1)^r\binom{n}{r}y^r x^s\varphi_s(n, r) \tag{B2}$$

Rearrange the left hand member and re-expand it, to get

$$\begin{aligned}[(1-x)-y(1+x)]^n &= [(1-y)-x(1+y)]^n \\ &= \sum_{s=0}^{n}(-1)^s\binom{n}{s}x^s(1+y)^s(1-y)^{n-s} \\ &= \sum_{s=0}^{n}\sum_{r=0}^{n}(-1)^s\binom{n}{s}x^s y^r \varphi_r(n,s)\end{aligned} \tag{B3}$$

Comparing coefficients of $x^s y^r$ in (B2) and (B3), we have, finally,

$$(-1)^r\binom{n}{r}\varphi_s(n,r) = (-1)^s\binom{n}{s}\varphi_r(n,s) \quad (n, r, s \text{ integers}), \tag{B4}$$

or, changing notation slightly,

$$\varphi_\xi(n-1,e) = (-1)^{\xi-e}\frac{\binom{n-1}{\xi}}{\binom{n-1}{e}}\varphi_e(n-1,\xi) \tag{B5}$$

(with n, e, ξ integers and $0 \leqq e, \xi \leqq n-1$). Thus if $\varphi_e(n-1,\xi)$ vanishes for e different integers ξ then so must $\varphi_\xi(n-1,e)$, at least when $e < n$. But $\varphi_\xi(n-1,e)$ is the coefficient of x^ξ in $(1+x)^e(1-x)^{n-1-e}$ when this is written out as a polynomial in x, by definition.

REFERENCES

1. R. W. Hamming, B.S.T.J., **29**, p. 147, 1950.
2. C. E. Shannon, B.S.T.J., **27**, p. 379, 1948.
3. P. Elias, Trans. I.R.E., **PGIT-4**, p. 29, 1954.
4. M. J. E. Golay, Trans. I.R.E., **PGIT-4**, p. 23, 1954.
5. D. Slepian, B.S.T.J., **35**, p. 203, 1956.
6. E. L. Ince, *Ordinary Differential Equations* (Dover), Ch. V, XV.
7. M. J. E. Golay, Proc. I.R.E., **37**, p. 637, 1949.
8. K. M. Case, Phys. Rev., **97**, p. 810, 1955.